California's New Data Privacy Law: New Thinking on Its Implications for Pharma

INTOUCH GROUP®

Executive Summary

Concerns about data privacy have grown in recent years after large-scale data breaches at hospitals, banks, retailers, and on social media platforms. In response, many governments have been developing legislation, among them, California, which passed the California Consumer Privacy Act (CCPA) in June 2018.

Although it is less all-encompassing than the European Union's General Data Protection Regulation (GDPR), California's is considered to be the most comprehensive law of its kind so far in the United States. However, while it goes into effect January 1, 2020, the law is still evolving through public hearings, amendments, and guidance.

In September 2018, we published an initial POV on this topic, called "Should Pharma Care About California's New Data Privacy Law?" in which we explained the legislation and provided recommendations for how pharma marketers can safeguard themselves against the likeliest consequences.

In the intervening months, we've been monitoring the legislative process and the discussions and reactions of opinion leaders. This POV is an updated version of the original, providing the latest thinking on this law and its implications for pharma marketers.

Overview

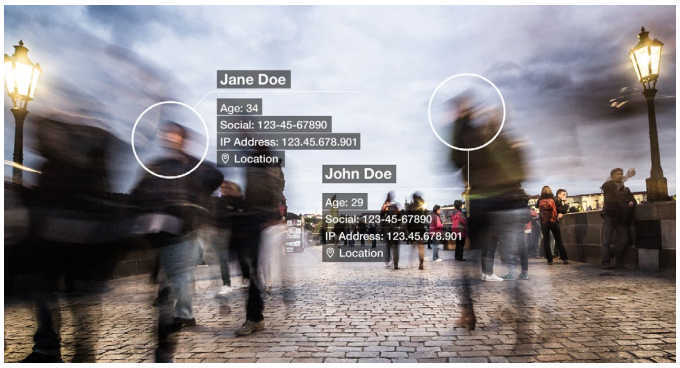
On June 28, 2018, California's governor signed the CCPA into law, which gives state residents greater control over the collection and use of their personal information. The CCPA goes into effect in January 2020. It gives consumers and the state Attorney General (AG) more authority to hold companies accountable for noncompliance.

California was the first state to pass a data-breach notification law; now all 50 states have one. It's been said that California leads the way for the rest of the United States in many regards — e.g., environmental protections, social and political movements, tech innovation — and it likely will lead with data privacy protections as other states follow suit.

What Rights Does the CCPA Grant to California Residents?

Under the CCPA, California residents have the right to:

- Know what personal information is being collected about them.
- Access their personal information.
- Know whether their personal information is disclosed, and if so, to whom.
- Know whether their personal information is shared, and if so, the right to opt out of certain sharing.
- Equal service and price regardless of whether they exercise their privacy rights.



What Is Considered "Personal Information" Under CCPA?

Personal information, under the CCPA, currently includes information that "identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." This is an expansive definition and may include the following example(s):

- Names
- Addresses

- Social security numbers
- Email and physical mailing addresses
- Geolocation
- IP addresses of all devices a consumer uses (i.e., smart phones, tablets, computers)
- Shopping or browsing history
- Psychological profiles
- Behaviors and attitudes
- Audio, electronic, visual, thermal, olfactory, and similar information
- Consumption behaviors and consumer preferences

Information exempt from the CCPA includes "protected health information that is collected by a covered entity or business associate governed by the privacy, security and breach notification rules issued by" the U.S. Department of Health and Human Services and governed by HIPAA. According to the International Association of Privacy Professionals, "The lawmakers extended the HIPAA/CMIA [Confidentiality of Medical Information Act] exemption to providers of healthcare governed under CMIA or covered entities governed by the specified federal privacy, security, and breach notification rules established pursuant to HIPAA, to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information." Ultimately, this means that exemptions in the CCPA are intended to prevent double regulation where an entity is already complying with a more rigorous privacy regime.

However, a business may qualify for the exemption for certain personal information that it collects or certain uses of personal information, but not qualify for the exemption under other circumstances. For example, the CCPA includes an exemption for "[i]nformation collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule . . . ." This exemption does not apply to information collected in a clinical trial that is not subject to the Common Rule (e.g., privately funded clinical trials).

What Kinds of Companies Are Affected?

CCPA affects any company doing business in California that meets at least one of the following criteria:

- You have more than $25MM in gross annual revenue
- You buy, hold, sell or share personal information of 50K consumers, and/or households or devices
- You derive at least 50% of your revenue from selling consumers' personal information

What Do Consumers Think?

A few years ago, we noted a 2014 Pew Research study in which experts predicted that by 2025, "the public will have lost the concept of privacy as we know it today." While that may have been the best minds forecasting at the time, that isn't coming to pass.

Consumers today are a little spooked, with two-thirds saying that current laws aren't providing adequate privacy protection. Cybersecurity firm RSA's second annual Data Privacy & Security Survey, conducted in early 2019, found that while the United States was the country surveyed with the greatest level of consumer acceptance of data sharing, the concept of privacy is of increasing concern.

> "[T]here is a growing disconnect between how companies capitalize on customer data and consumer expectations around how their data should be used and secured. 2018 was host to a myriad of high-profile data breaches that compromised billions of accounts. … While consumers believe there are ethical ways companies can use their data, they harbor heightened concerns about their privacy, distrust trends such as personalization and device tracking, and blame companies when hacked."
> – RSA Data Privacy & Security Survey, 2019

It's only been just over a year since the European Union's GDPR went into effect, but according to one recent article, "the U.K.'s data privacy watchdog says that the number of complaints it has received under GDPR has nearly doubled, and [as more people become aware of their rights] the trend is expected to continue." If EU consumer response to the

GDPR is any indication, U.S. attitudes about privacy may shift and demands for greater protections may gain momentum, particularly as CCPA puts a spotlight on privacy for Americans.

Is California the Only State Enacting Privacy Laws?

Several states around the country have also recently put into place, or amended, privacy laws, including Nevada, Alabama, Colorado, Oregon, Louisiana, Vermont, and Virginia. Of note, Nevada enacted legislation (Nevada Senate Bill 220) on May 30, 2019 that provides consumers with a right to opt out of the sharing of personal information.

As of today, there are over a dozen CCPA-like "copycat" bills at various stages of consideration in legislatures across the United States.

CCPA: A Law With Issues

As the American Association of Advertising Agencies (4A's) has **pointed** out in public-hearing testimony to the California AG, parsing and preparing for CCPA is proving particularly challenging for several reasons, including:

- Ambiguity and lack of clarity on points that could create situations of confusion or contradiction.
- Internal contradictions, such as the potential to require more data to verify consumer requests for data deletion.
- Concerns related to treating pseudonymized data as equivalent with personal information.

The AG has said that they are targeting the fall of 2019 to **publish** draft rules related to the legislation. Additionally, about a dozen amendments are pending, which aim to solve some of the noted challenges.

For example, AB-873 clarifies the definition of personal information to stipulate that it must be "reasonably linkable" to a consumer, and to define de-identification to include data that is not "reasonably linkable."

Lawmakers have already amended the CCPA with an exemption for clinical-trial data. Additional adjustments may do more to help clarify the law, but only time will tell.

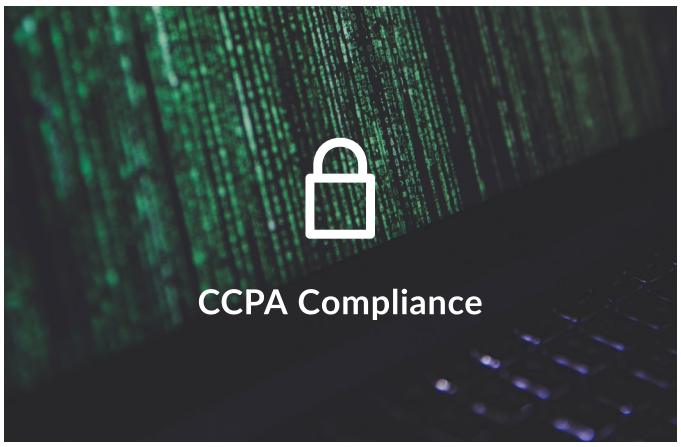
Some Implications for Pharma

The law is likely to be amended and is subject to change in the coming months. This is important to keep in mind. Nonetheless, there are several points of especial note for pharma marketers, which include the following:

01. In its current form, when the law goes into effect, the consumer can request their last 12 months of data. To comply with this "look back period," companies should begin reviewing current practices for collecting, using, and sharing personal information.

02. Currently, pseudonymous identifiers, such as unique IDs that mask personal information, can be considered personal information. This could require reviewing processes for storing data to ensure personal information has been appropriately anonymized for purposes of the CCPA. If anonymization is not possible, steps should be taken to ensure that the use of such data is handled appropriately.

03. The CCPA defines three categories of affected parties: businesses, service providers, and third parties. Each has different responsibilities under the law. An organization's classification — and its legal liabilities — could change depending on how it uses and shares personal information under different circumstances.



Recommendations for CCPA Readiness

The CCPA doesn't go into effect until January 1, 2020, and more changes to it may be made, but why wait to make sure you're compliant? Initial steps include:

- Consulting with your legal team to determine the applicability of the CCPA (and to the extent whether any exemptions apply) and to develop a prioritized action-item list based on your organization's biggest risks.
- Creating an inventory (also known as a data map) of your data and auditing your privacy practices to determine how your company (and your partners at agencies, clients, and vendors) collect, use, disclose, sell, or share personal information.
- Reviewing agreements with your partners, clients, and vendors to determine whether any provisions need to be added to address CCPA requirements.
- Implementing the necessary technology and process changes necessary to comply with the CCPA in terms of verifying and accommodating consumer requests and storing and managing data. And, after implementing the changes, testing them and proving them in action.
- Updating privacy policies and notices.
- Creating an internal training plan, if appropriate.

Conclusion

The CCPA gives California consumers a new level of control over their personal information. As concerns over data security and privacy grow, it's likely that other states, regions, and nations will follow and create or expand their privacy protections. Intouch will continue to monitor this issue.

This legislation is still a moving target: amendments are pending, and guidelines are yet to be released. However, many actions can and should still be begun immediately to prepare wisely for this and other privacy issues. Ensuring regulatory compliance is paramount in our industry on many fronts, from manufacturing to marketing — and data privacy is no different. Reach out to your Intouch team today to help make sure your brand is covered.

Author: Intouch Team

Want to learn more about CCPA?
Contact Brady Walcott at 214.642.5290
brady.walcott@intouchg.com
intouchg.com